UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
KNOXVILLE

IN THE MATTER OF THE SEARCH OF: DESKTOP COMPUTER IN A BLACK COSAIR CASE S/N: 089314528804, WITH STICKER FOR "DIGITAL STORM CUSTOMIZED SYSTEMS", S/N: 6102APRIL 54225, CURRENTLY STORED AT THE KNOXVILLE FEDERAL BUREAU OF INVESTIGATION, 1501 DOWELL SPRINGS BLVD., KNOXVILLE, TENNESSEE 37909.

Case No. 3:20-MJ- 2248

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Emily Ciaravino, being duly sworn, state the following information to be true to the best of my knowledge, information and belief:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") and have been so employed since January 2019. I am an "Investigative or Law Enforcement Officer" within the meaning of Section 2510(7) of Title 18, United States Code; that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code. My primary duties and responsibilities involve the investigation of violations of federal law including violent crime as found in Title 18 of the United States Code and the Controlled Substances Act as found in Title 21 of the United States Code.

2. I am currently assigned to the Knoxville Field Office of the FBI and am assigned to the Violent Crime Squad. During my tenure as a Special Agent, I have investigated crimes including, but not limited to, bank robbery, gangs and organized crime, narcotics trafficking, fugitive investigations and violent crimes against children. More specifically, I have investigated

violent crimes against children conducted both physically and via the internet. I have conducted physical surveillance, assisted in the execution of search warrants, analyzed phone and internet records, and conducted arrests of criminal subjects.

3. Prior to joining the FBI, I was a Detective in the Criminal Investigations Division of the Roane County Sheriff's Office in Roane County, Tennessee. I received several hours of training and attended numerous classes regarding investigative techniques and methods related to crimes against children. Throughout that time, I drafted, executed and participated in several search warrants regarding social media accounts and electronic devices specifically related to crimes against children.

4. I make this affidavit in support of an application for a search warrant for the Desktop Computer in a black Cosair Case, S/N: 089314528804, with a sticker for "DIGITAL STORM CUSTOMIZED SYSTEMS", S/N: 6102APRIL 54225, seized from the residence of Matthew Paul Bajaj after obtaining written consent. The desktop computer is currently stored at the Knoxville Federal Bureau of Investigation, 1501 Dowell Springs Blvd, Knoxville, Tennessee 37909. I seek authorization to search the aforementioned computer for the items specified in Attachment B, incorporated with this affidavit, which constitute contraband, evidence, fruits and instrumentalities of, and property designed for use in committing violations of 18 U.S.C. § 1201 (kidnapping), 18 U.S.C. § 2423(a) (transportation with intent to engage in criminal sexual activity), and 18 U.S.C. § 2423(b) (interstate travel for the purpose of engaging in illicit sexual conduct).

5. The statements contained in this affidavit are based my investigation; information provided by FBI Special Agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents; information gathered from

the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent with the FBI. Because this affidavit is being submitted for the limited purpose of securing authorization for the requested search warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband, evidence, fruits, and instrumentalities of, and property designed for use in committing violations of 18 U.S.C. § 1201 (kidnapping), 18 U.S.C. § 2423(a) (transportation with intent to engage in criminal sexual activity), and 18 U.S.C. § 2423(b) (interstate travel for the purpose of engaging in illicit sexual conduct).

DEFINITIONS

6. The following definitions, inclusive of all definitions contained in 18 U.S.C. § 2256, apply to this affidavit and Attachment B:

a. "Computer" refers to any electronic, magnetic, optical, electrochemical, or other high-speed data processing device capable of performing logical or storage functions, and includes any data storage facility or communications facility directly related to such a device. As used herein, "computer" also incorporates digital devices that complete these same functions, such as smartphones, tablets, connected devices, and e-readers. See 18 U.S.C. § 1030(e)(1).

b. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-

processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

c. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

d. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider assigns a different unique number to a computer every time it accesses the Internet. IP addresses may also be static, which means the

provider assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

e. "Mobile applications" or "mobile apps" are computer programs or software applications specifically designed to run on mobile devices (e.g., smartphones, tablets, e-readers, etc.). Mobile applications are generally downloaded from application distribution platforms operated by specific mobile operating systems, like App Store (Apple mobile devices) or Google Play Store (Android mobile devices).

f. "Instant messaging" is a type of communication that offers real-time text transmission over the Internet. Instant messaging generally involves short messages which are transmitted between two or more parties. Various social networking, dating and gaming websites and mobile applications offer instant messaging for users to communicate amongst themselves. More advanced features of instant messaging include push technology to provide real-time text, and the ability to send/receive digital files, clickable hyperlinks, and video chat.

g. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data(and any photographic form.

SPECIFICS REGARDING THE SEARCH AND SEIZURE OF COMPUTERS

7. Based on my training and experience, I am aware that the search of computers often requires agents to seize most of the computer items (e.g., hardware, software, and instructions) to

be processed later by a qualified computer expert in a laboratory or other controlled environment. That is essential to the search for electronic evidence because of the following facts:

a. Computer storage devices, like hard drives, diskettes, tapes, or laser disks, store the equivalent of thousands of pages of information. When the user wants to conceal electronic evidence of a crime, he or she may store it in random order with deceptive file names. This requires searching authorities to examine all of the stored data to determine whether it is included within the scope of warrant. This process can take weeks or months, depending on the volume of the stored data, and it would be impractical to attempt this kind of data search on-site;

b. Searching computer systems for criminal evidence is a highly technical process that requires expert skills and a properly controlled environment. The vast array of computer hardware and software available today requires even computer experts to specialize in specific systems and applications. It is difficult to know prior to a search which expert should analyze the system and its data. The search of a computer system can be equated to a scientific procedure, which is designed to protect the integrity of the evidence while recovering hidden, erased, compressed, password-protected, and other encrypted files. Because computer evidence is extremely vulnerable to tampering and destruction, both from external sources and from code embedded in the system as a "booby-trap," the controlled environment of a laboratory is essential to its complete and accurate analysis;

8. The facts set forth in this affidavit establish probable cause to believe that a computer, its storage devices, and other system components were used as a means of committing offenses involving kidnapping, the transportation of a minor to engage in sexual activity and

interstate travel for the purpose of engaging in illicit sexual conduct. Accordingly, I seek the authorization to search the computer listed in Attachment A, consistent with Attachment B to the requested warrant.

PROBABLE CAUSE

9. On October 28, 2020, at approximately 8:31 a.m., the Oak Ridge Police Department ("ORPD") received a report that a 12-year-old female, hereinafter referred to as "Victim," and whose identity is known to law enforcement, was missing from her residence, located at 101 Mississippi Avenue, Oak Ridge, Tennessee. The Victim was reported missing by her mother, Kelly McManus. The Victim was last seen the night before, inside her residence, which is located within the Eastern District of Tennessee. The Victim was last seen wearing a red and black flannel shirt, black jeans, black and white Nike shoes, and costume cat ears.

10. Telephone records indicated the Victim's cellular telephone had been in contact with telephone number 828-719-0114, and had a 103-minute call with that number on October 27, 2020. ORPD detectives obtained subscriber information for the phone number associated with Matthew Paul Bajaj of 24 Oakcrest Place, Asheville, North Carolina 28806, hereinafter referred to as "Bajaj." ORPD detectives identified Bajaj as a 42-year-old male with a North Carolina Driver License. Bajaj is the registered owner of a blue 2013 Subaru Impreza Limited, bearing North Carolina license plate number ME0WBP. ORPD detectives conducted an inquiry of the ORPD License Plate Reader (LPR) system which captures images of vehicles entering Oak Ridge and stores the associated information which can be queried at a later time by license plate or vehicle description. Law enforcement discovered Bajaj's vehicle was recorded in ORPD's LPR database on October 5, 2020, October 12, 2020, and October 21, 2020. On October

27, 2020, a vehicle matching the description of Bajaj's vehicle was captured in the area of South Illinois Avenue in Oak Ridge, Tennessee at approximately 6:53 p.m., which was just prior to the time Bajaj checked into the Double Tree Hotel. The LPR system was not able to decipher the license plate of the vehicle, but a manual review of the vehicle and license plate was conducted by law enforcement officers. The manual review confirmed the vehicle belonged to Bajaj.

11. On October 28, 2020, ORPD obtained an exigent authorization for geo-location information of the Victim's cellular telephone through the cellular service provider. The Victim's cellular telephone geo-located within the vicinity of the Double Tree Hotel, 215 S. Illinois Avenue, Oak Ridge, Tennessee, at approximately 10:00 a.m. on October 28, 2020. Law enforcement officers confirmed Bajaj booked room number 413 at the Double Tree Hotel in Oak Ridge, Tennessee on October 27, 2020, and had the room rented until October 29, 2020. Bajaj paid for the room utilizing a bank card with his name and the last four digits 9988. It was learned that Bajaj had rented a room at the Double Tree Hotel on October 10, 2020 and on October 20, 2020 utilizing the same bank card with the last four digits of 9988.

12. On October 28, 2020, at approximately 12:00 p.m., ORPD officers made entry into room number 413 at the Double Tree Hotel in an attempt to recover the Victim. Officers did not locate the Victim and determined the room was vacant. While securing room number 413, officers saw in plain view, a Kroger grocery bag and a phone charger, as well as sheets on the bed that had not been made.

13. On October 28, 2020, the Tennessee Bureau of Investigation and the ORPD obtained and executed a search warrant of the Double Tree Hotel room 413 where Bajaj and the Victim spent the night of October 27, 2020. Inside the hotel room was a receipt from a business, Vavavoom LLC, located at 57 Broadway Street, Asheville, NC 28801 where Bajaj purchased the

following items: UBERLUBE Good to Go Silver, UBERLUBE 50ml, Bijoux MAZE SINGLE CHOKER, FF Deluxe Silky Rope and Lux Fetish Eye Mask which totaled $142.31 paid for with a debit card with the last four digits 9988. These last four digits are the same as the card utilized to purchase Double Tree Hotel room 413. Inside the Hotel room, law enforcement located the packaging associated with a Fetish eye mask, Fetish deluxe silky rope and Uberlube Good to Go Silver. A dark colored paper bag was located in the trash can inside the hotel room labeled "Vavavoom Apparel, Lingerie and Safe-Sex Toys".

14. Law enforcement officers reviewed video surveillance footage at the Double Tree Hotel. Officers were able to verify that Bajaj checked into the Double Tree Hotel on October 27, 2020, at approximately 7:00 p.m. Bajaj was wearing a grey t-shirt with what appeared to be black and white cats, khaki shorts, a dark colored baseball style hat, a black facemask, black glasses, and had on a black and blue backpack. Bajaj was holding one white tote bag with the Logo "Box Linch" and one black tote bag. Officers observed Bajaj leave the hotel and return at approximately 10:30 P.M. on October 27, 2020. Law enforcement officers observed Bajaj arrive in the parking lot of the Double Tree Hotel driving a blue 2013 Subaru. Law enforcement officers also observed a female, now identified as the Victim, with Bajaj on the surveillance video. The female was wearing a red flannel jacket, costume cat ears on her head, black jeans and had dark colored hair, which was consistent with the description the Victim's clothing when she was last seen at her residence. Based on the surveillance video, law enforcement officers believed the female was the Victim. Law enforcement officers spoke with the Double Tree Hotel desk clerk who was working during the night of October 27, 2020, and he recalled seeing Bajaj and the female.

15. Law enforcement officers went to the Kroger grocery store in Oak Ridge, Tennessee and obtained surveillance video footage depicting Bajaj and the Victim with dark hair, wearing a red flannel shirt, walking around Kroger at approximately 10:00 p.m. on October 27, 2020. Law enforcement officers at the Double Tree Hotel also viewed surveillance video footage of Bajaj and the Victim wearing the flannel shirt coming into the Hotel shortly after they were seen on the Kroger surveillance video.

16. Law enforcement officers viewed surveillance video footage of Bajaj at Books A Million in Oak Ridge, Tennessee where he made a transaction on October 28, 2020 at approximately 10:08 a.m. Bajaj was seen on the surveillance video footage wearing a green shirt, shorts, dark shorts and sandals.

17. Law enforcement officers obtained an exigent authorization for geo-location information for Bajaj's cellular telephone through his cellular service provider. Based on this information, law enforcement was alerted to the location of Bajaj's cellular telephone which was within the vicinity of his residence, located at or near 24 Oakcrest Place, Asheville, North Carolina.

18. On October 28, 2020, your affiant contacted FBI agents in Asheville, North Carolina, advised them of the situation, and requested they respond to Bajaj's residence. FBI agents and officers from the Asheville Police Department ("APD") responded to Bajaj's residence and observed Bajaj's blue 2013 Subaru, bearing North Carolina license plate number ME0WBP, parked in front of the residence. Located inside the vehicle in plain view was a Books-A-Million plastic bag.

19. On October 28, 2020, at approximately 4:13 p.m., FBI agents and APD officers conducted a "knock and talk" at Bajaj's residence. Bajaj came to the door and was asked to step

outside by law enforcement. Bajaj exited his residence and was asked if the Victim was inside his residence, and if she was okay. Bajaj confirmed the Victim was okay and was inside of his residence. FBI Supervisory Special Agent ("SSA") William Gang asked Bajaj if agents could enter his residence. Bajaj said something similar to, "I guess so." SSA Gang entered Bajaj's residence and called the Victim's name 2-3 times and identified himself as law enforcement. The Victim exited a room down a hallway and met SSA Gang near the entrance of the residence.

20. Bajaj was taken into custody and voluntarily interviewed by law enforcement officers. Additionally, Bajaj provided written consent to FBI agents to execute a search of his residence, Motorola cellular phone, associated with the cellular telephone number (828) 719-0114, and his personally owned Windows Desktop computer which was located inside of his residence.

21. During the interview, Bajaj admitted to having sexual intercourse with the Victim at the Double Tree Hotel in Oak Ridge, Tennessee. Bajaj stated he brought condoms, but did not use them when having sexual intercourse with the Victim. Bajaj admitted he had traveled to Oak Ridge on more than one occasion and had sex with the Victim. Bajaj stated he was not aware the Victim was a minor. Bajaj told agents he had been communicating with the Victim on his Windows 10 Digital Storm Customized Systems desktop computer and Motorola cellular telephone, utilizing social media applications, phone calls and text messages. Bajaj provided written consent to search the aforementioned devices he utilized to communicate with the victim.

22. Since the beginning of October Bajaj admitted he has lived by himself the past three months at his home. It is understood Bajaj works at Game Stop, a video game store.

23. After the custodial interview, the agents returned to Bajaj's residence to seize the desktop computer and Motorola cellular telephone. The cellular telephone was located on the

nightstand next to Bajaj's bed and the desktop computer was located in a room arranged like an office. FBI agents seized Bajaj's cellular telephone and desktop computer from his residence. When FBI agents were at the residence, they noticed a computer tablet in the kitchen and additional other electronic devices and electronic storage devices throughout the house. While at the residence, the agents also returned Bajaj's wallet, leaving it on the kitchen counter. When the wallet was left on the counter, a keycard from a hotel fell out of Bajaj's wallet.

24. The Victim's mother, Kelly McManus, stated that Bajaj was not related to the family and did not have legal custody of the Victim.

CONCLUSION

25. Based on the information set forth in this affidavit, there is probable cause to believe that contraband, evidence, fruits, and instrumentalities of, and property designed for use in committing violations of 18 U.S.C. § 1201 (kidnapping), 18 U.S.C. § 2423(a) (transportation with intent to engage in criminal sexual activity), and 18 U.S.C. § 2423(b) (interstate travel for the purpose of engaging in illicit sexual conduct) are located on the desktop computer in a black Cosair case, S/N: 089314528804, with a sticker for "DIGITAL STORM CUSTOMIZED SYSTEMS", S/N: 6102APRIL 54225, seized from the residence of Matthew Paul Bajaj, currently stored at the Knoxville Federal Bureau of Investigation at 1501 Dowell Springs Blvd., Knoxville, Tennessee 37909, as described in Attachment A, and the digital media therein. Accordingly, I respectfully request that this Court authorize the search of this residence so that agents may seize the items listed in Attachment B.

Emily Ciaravino
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on this 3 day of November, 2020.

HONORABLE H. BRUCE GUYTON
UNITED STATES MAGISTRATE JUDGE

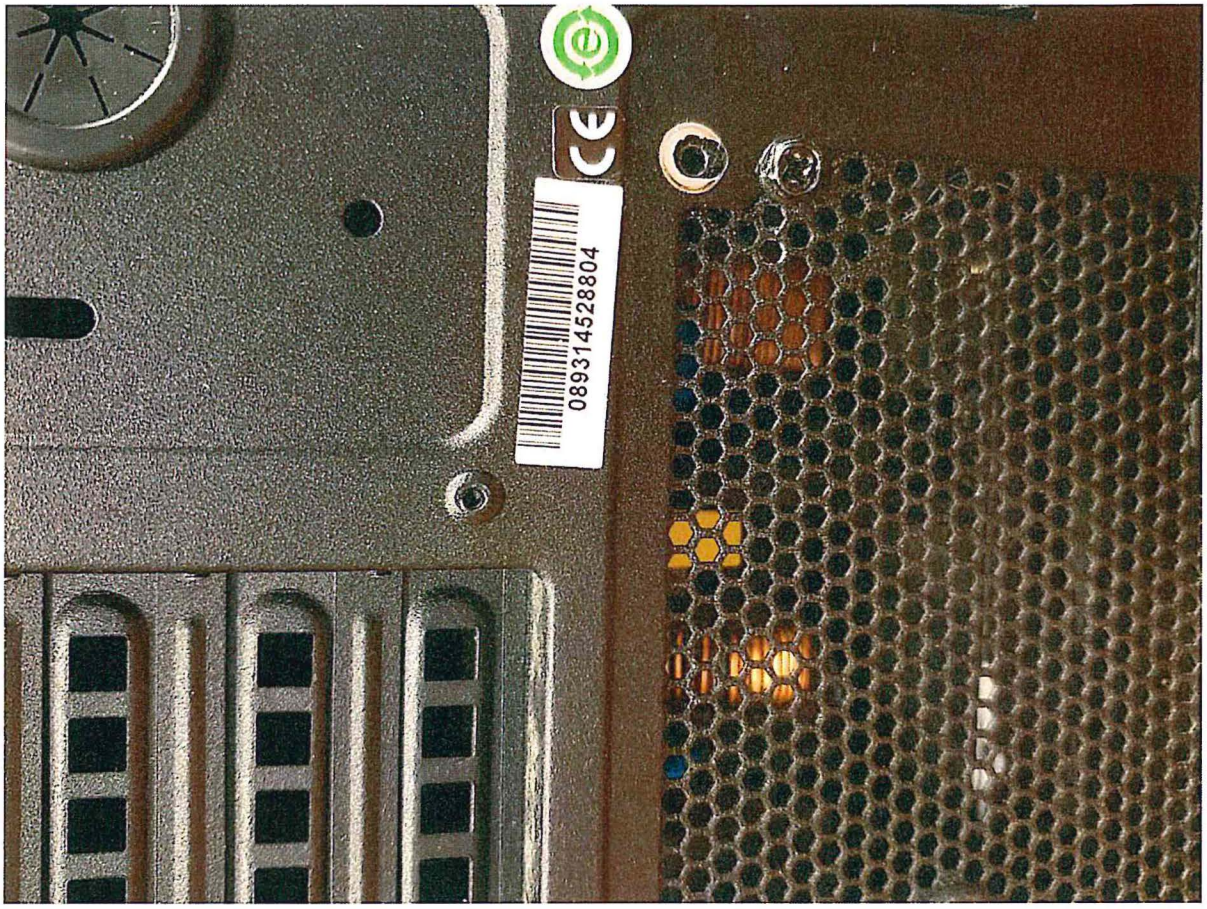
ATTACHMENT A

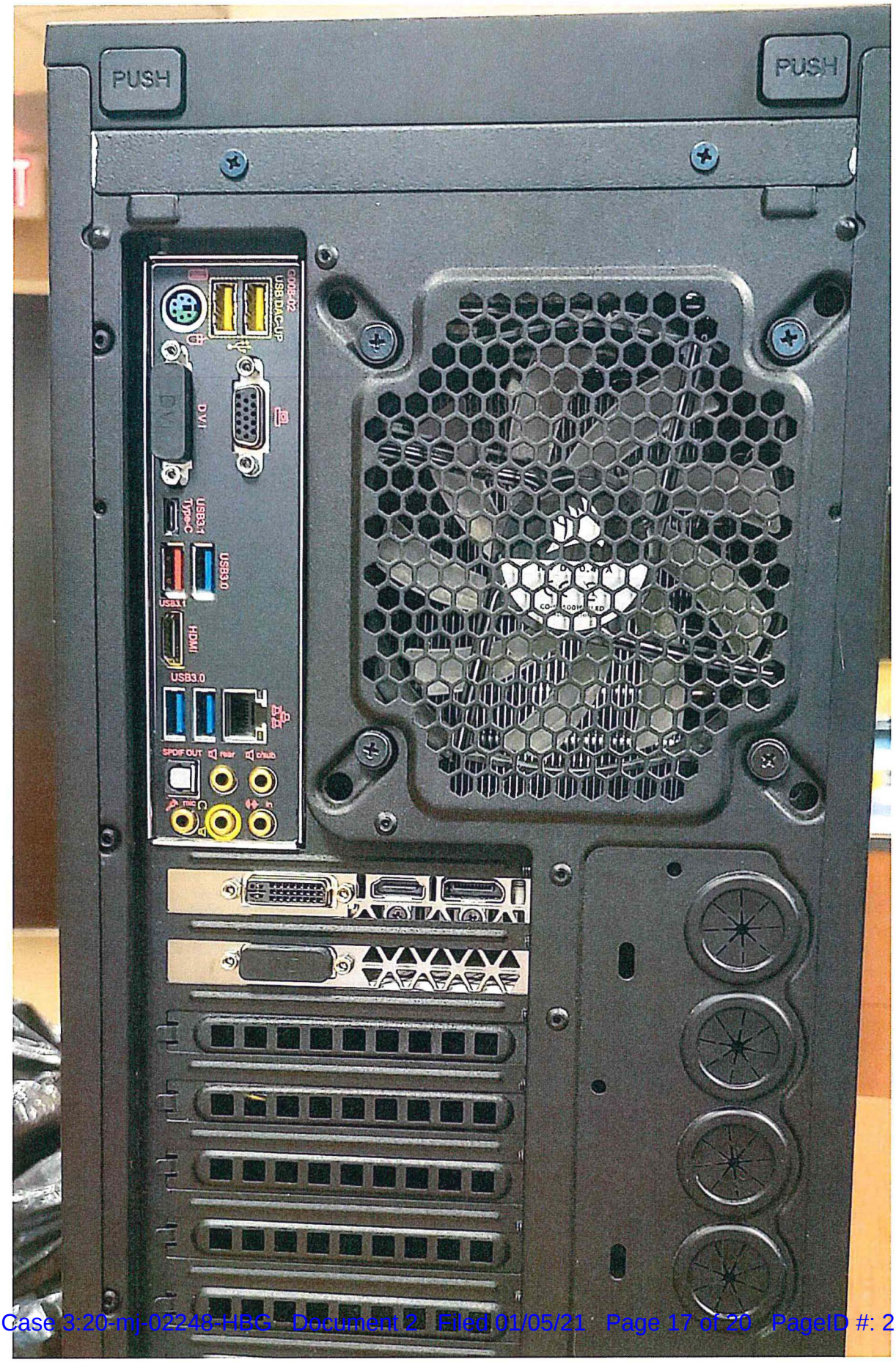
DESCRIPTION OF PROPERTY TO BE SEARCHED

Property: Desktop Computer in a black Cosair Case
S/N: 089314528804
With a sticker for "DIGITAL STORM CUSTOMIZED SYSTEMS"
S/N: 6102APRIL 54225

Location: Knoxville Federal Bureau of Investigation
1501 Dowell Springs Blvd., Knoxville, Tennessee 37909


DIGITALSTORM
CUSTOMIZED SYSTEMS
S/N:6102APRIL 54225


089314528804


PUSH
PUSH
PS/2
USB DAC-UP
DVI-I
USB3.1 Type-C
USB3.0
USB3.1
HDMI
USB3.0
LAN
SPDIF OUT
rear
chub
mic
in

ATTCHMENT B
PARTICULAR THINGS TO BE SEIZED
SPECIFICALLY DURING THE DATES OF OCTOBER 1, 2020 THROUGH OCTOBER 31, 2020

1. Any and all images of the Victim.

2. Any and all communication between Bajaj and Victim.

3. Records of social media sites utilized to communicate with the victim.

4. Evidence identifying the individual(s) who used, owned, or controlled the computer(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, accounts of Internet Service Providers.

5. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

6. Evidence of the lack of such malicious software.

7. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence.

8. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER.

9. Evidence of the times the COMPUTER was used.

10. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER.

11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital

data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

12. Travel documents and indicia of travel, including airline tickets, hotel records, reservations, and travel itineraries.

13. Evidence indicating the user's state of mind as it relates to the criminal violations under investigations (identified above).

14. Records of Internet Protocol addresses used;

a. Records of internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet or P2P search engine, and records of user-typed web addresses.

15. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.